



FORTINET®



FortiToken Mobile for Android

Release Notes

VERSION 4.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<http://kb.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING AND CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com/>

FORTIGUARD CENTER

<https://fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>



6/28/2018

FortiToken Mobile for Android Release Notes

33-440-497677-20180628

TABLE OF CONTENTS

Introduction	4
What's new	5
Product support	6
Android version support	6
FortiOS and FortiAuthenticator support	6
FortiToken platform scalability	6
Registering FortiToken Mobile	8
Resolved issues	9
Known issues	10

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiToken Mobile for Android, version 4.4.0, build 0086.

FortiToken Mobile is an OATH compliant, time-based one-time password (OTP) generator application for mobile devices. FortiToken Mobile produces its OTP codes in an application that you can download to your Android, iOS, or Windows mobile device without the need for a physical token.

Go to the Google Play store to download the free [FortiToken Mobile application](#) for Android.

For additional documentation, please visit: <http://docs.fortinet.com/fortitoken/>

What's new

Before upgrading, review the following changes for impact to your unique deployment. Note that this release includes just a few feature enhancements.

- Updated FortiToken Mobile PIN policy to always enforce strongest policy set by the FortiAuthenticator.
- Full Chinese language support.
- Various bug fixes.

Product support

Android version support

The following Android versions are supported:

- 4.4.x
- 5.x
- 6.x
- 7.x
- 8.x

The application works after the Android OS upgrades from:

- 4.x to 5.x
- 6.x to 7.x
- 7.x to 8.x

FortiOS and FortiAuthenticator support

FTM requires FortiOS 5.4 and 5.6 and/or FortiAuthenticator 5.0 and 5.1.

FortiToken platform scalability

The following table shows the maximum number of FortiTokens that can be assigned to certain FortiGate and FortiAuthenticator models. Note that FortiToken is also supported on specific FortiWiFi models.

All data for this table was taken from the following [Product Matrix datasheet](#).

FortiGate Models	Max. FortiTokens
30E	20
50E / 60D / 60E / 70D / 80D / 90D / 90E	100
100D / 100E / 200D / 200E / 300D / 500D / 600D / 800C / 900D	1,000
1000D / 1200D / 1500D / 2000E / 2500E / 3000D / 3100D / 3200D / 3700D / 3800D / 7040E	5,000
VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	

FortiAuthenticator Models	Max. FortiTokens
200E	500
400E	2,000
1000D	10,000
2000E	20,000
3000D / 3000E	40,000
VM BASE to VM-100000-UG	200 to 200,000+

Registering FortiToken Mobile

You will need a certificate to register FortiToken Mobile. There are two options for getting FortiToken Mobile certificates for use on your authentication server: FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

For each FortiToken Mobile purchase, you will receive a physical redemption certificate. Scratch off the designated area of the redemption certificate to reveal the 20-digit activation code.

The following steps show how to register FortiToken Mobile on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Locate the 20-digit code on the redemption certificate.
2. Go to **User & Device > FortiTokens** and select **Create New**.
3. Select **Mobile Token**, and enter the 20-digit certificate code in the **Activation Code** box.
4. Select **OK**.

On the FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to **Authenticator > User Management > FortiTokens** and select **Create New**.
3. Select **FortiToken Mobile**, and enter the 20-digit certificate code in the **Activation codes** box.
4. Select **OK**.

To ensure messaging functions properly, you must configure the messaging server, configure users to receive messages from the server by email or SMS, and provision FortiToken Mobile for the user on the FortiGate and/or FortiAuthenticator.

To see more information on how to provision FortiToken Mobile for a user on a FortiGate and FortiAuthenticator, see the [FortiToken Mobile - User Instructions](#).

For more information see the FortiToken Mobile product datasheet available on the Fortinet web site at <https://www.fortinet.com/products/identity-access-management/fortitoken-mobile.html>.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release.

For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
461605	Error when transferring multiple tokens.
462676	One token value is missing if two tokens are transferred from two different users or the same user.
421376	Application crashes when opened.
493833	Minor Chinese translation issues.
472036	HOTP displays then disappears.
445104	Background screen issues for detailed push log when FortiToken Mobile is on the fingerprint ID authentication view and sends push.
480477	FortiToken Mobile PIN policy to always enforce the strongest policy set on a FortiAuthenticator.
440339	Cannot proceed after fingerprint ID screen.
417420	Display the message "Authenticate with pin (or touch ID) to complete login" on expanded push notifications when authentication is required by iOS or application and the user approves the login request.
460186	FortiToken Mobile application crashes on Nexus 5x (Android 8).
440125	Push notifications incorrectly displayed when application is running in the background.
408308	Application crashes when sending push on HOTP.
417440	User can deny login attempts without having to pass authentication.
410935	Application crashes after upgrade when testing "Enable Touch ID" and back button.
416888	Bypass pin and touch ID feature.
408297	Application crashes on Android S7.
460968	Login request dialog on tablet changed.
486626	"No FortiAuthenticator IP found" error should not show for SSL VPN users.

Known issues

This section lists the known issues of this release, but is not a complete list.

For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
483880	Differentiate tokens issued by request from FortiToken Cloud.
459946	Push dialog flashes before the fingerprint ID authentication.
472252	Support new field in API call to FortiAuthenticator to get token transfer activation code.
484791	FortiToken Mobile cannot transfer previously activated tokens after upgrading FortiAuthenticator.
480797	Handle new "Display_Name" field in push payload.
496955	"Cannot transfer tokens issued by FortiGate" message should use singular "token".
493825	"Please check your network connectivity" error appears when transferring tokens.
480017	"Login Validation FAILED ftm_id" error appears when approving login attempt.
483026	"No data from server" error appears when SSL VPN user's login attempt has been approved.
476539	"Please wait" message doesn't disappear after connection is timed out.
477733	Should disable "transfer token" option if FortiToken Mobile has a token from FortiAuthenticator pre 5.2.



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.